UNITED STATES DISTRICT COURT

for the

Northern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The Premises Located at 520 W. Oneil St., Dublin, Texas 76446 and the person of Christopher David Mayhall

Case No. 4:19-MJ-101

[FILED UNDER SEAL]

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The Premises Located at 520 W. Oneil St., Dublin, Texas 76446 and the person of Christopher David Mayhall, as further described in attachment A.

located in the Northern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2251	Sexual exploitation of children;
18 U.S.C. § 2252	Production, possession, receipt and/or distribution of child pornography.
18 U.S.C. § 2252A	

The application is based on these facts:

See attached affidavit of Special Agent Jacob R. Downing.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Jacob R. Downing, Special Agent FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 1/31/19

Judge's signature

City and state: Fort Worth, Texas

Jeffrey L. Cureton, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Jacob R. Downing, a Special Agent with the Federal Bureau of Investigation, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as a Special Agent of the Federal Bureau of Investigation (FBI) since September 2015, and I am currently assigned to the Dallas Division. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I am currently assigned to a Resident Agency, wherein my duties and responsibilities include investigating criminal violations relating to the sexual exploitation of children (SEOC).

2. I submit this application and affidavit in support of a search warrant authorizing a search of 520 W. Oneil St., Dublin, TX 76446, (the "premises") and the person of Christopher David MAYHALL ("MAYHALL"), as further described in Attachment A incorporated herein by reference. As will be shown below, there is probable cause to believe that Christopher David MAYHALL, an individual living at 520 W. Oneil St., Dublin, TX 76446, has attempted to produce, has possessed, transported, and/or distributed child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. Located within the premises and person to be searched, I seek to seize evidence and instrumentalities of criminal violations, which relate to the attempted production, knowing possession, transportation and distribution of child pornography.

I request authority to search the entire premises, including all residential dwellings, storage buildings and any computer and computer media located therein, as well as the person of Christopher David MAYHALL for items specified in Attachment B (which is incorporated herein by reference) which may be found, and to seize all items listed in Attachment B as instrumentalities and evidence of a crime, all located within the Northern District of Texas, Fort Worth Division.

3. Additionally, I am aware that many computers and electronic storage devices today, such as laptop computers, tablets, telephones, external drives and thumb drives, are portable. I also know from my training and experience that these devices are often stored in vehicles to prevent other users in the home from discovering the existence of the child pornography collection. Therefore, this application seeks permission to search vehicles located at on the premises and/or its curtilage that fall under the dominion and control of the person or persons associated with said premises. The search of these vehicles is to include all internal and external compartments and all containers that may be associated with the storage of child pornographic materials or their instrumentalities contained within the aforementioned vehicles.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence and instrumentalities of the violation of 18 U.S.C. §§ 2251, 2252 and 2252A,

are presently located at 520 W. Oneil St., Dublin, TX 76446. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of 18 U.S.C. §§ 2251, 2252 and 2252A, relating to material involving the sexual exploitation of minors.

a. 18 U.SC. § 2251(a) prohibits a person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, knowing or having reason to know that such visual depiction will be transmitted or transported using any means or facility of interstate commerce.

b. 18 U.S.C. § 2251(d)(1)(A) prohibits a person from knowingly making and publishing, or causing to be made and published, any notice offering to exchange, display, distribute, and reproduce and visual depiction of child pornography.

c. 18 U.S.C. § 2252(a)(1) prohibits knowingly transporting or shipping, using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mails, any visual depiction of minors engaging in sexually explicit conduct.

d. 18 U.S.C. § 2252(a)(2) prohibits knowingly receiving or distributing, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been

mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct.

e. 18 U.S.C. § 2252(a)(4) prohibits possessing or knowingly accessing with intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means, including by computer, if the producing of such visual depiction involved the use of a minor engaging in sexually explicit conduct and the visual depiction is of such conduct.

f. 18 U.S.C. § 2252A(a)(1) prohibits knowingly mailing, transporting, or shipping any child pornography using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer.

g. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing any child pornography that has been mailed, or using any means or facility or interstate commerce, shipped or transported in or affecting interstate or

foreign commerce by any means, including by computer; or knowingly receiving or distributing any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

h. 18 U.S.C. § 2252A(a)(3)(A) prohibits a person from knowingly reproducing child pornography for distribution through the mails, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

i. 18 U.S.C. § 2252A(a)(3)(B) prohibits knowingly advertising, promoting, presenting, distributing, or soliciting through the mail, or using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer, any material or purported material, in a manner that reflects the belief or is intended to cause another to believe, that the material is or contains a visual depiction of an actual minor engaging in sexually explicit conduct, or an obscene visual depiction of a minor engaging in sexually explicit conduct.

j. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view, any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported using any

means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B:

a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).

c. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility

directly related to or operating in conjunction with such device." See 18 U.S.C. § 1030(e)(1).

d. "Computer Server" or "Server," as used herein, is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet.

e. "Computer hardware" consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

g. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. It commonly includes programs to run operating systems, applications, and utilities.

i. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

j. "Internet Service Providers" (ISPs), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

k. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored

both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

l. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

m. "Minor" means any person under the age of 18 years. See 18 U.S.C. § 2256(1).

n. "Preview image" refers to an image or a set of images that is a representative sample of a larger collection of images or video(s). Preview images are commonly used to advertise the content of materials that are available at another internet location.

o. "Peer-to-peer file-sharing" (P2P) is a method of communication available to Internet users through the use of special software. Computers link together through the Internet using this software, which allows sharing of digital files between users on the same network.

A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting searches for files that are currently being shared on another user's computer.

p. "Sexually explicit conduct" applies to visual depictions that involve the use of a minor, see 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, see 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. See 18 U.S.C. § 2256(2)(A).

q. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. See 18 U.S.C. § 2256(5).

r. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers

to various web clients via Hyper-Text Transport Protocol (HTTP).

s. "Imaging" or "copying" refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents but attributes may change during the reproduction.

t. "Hash value," or "SHA-1," refers to a mathematical algorithm generated against data to produce a numeric value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated. Hash values cannot be used to find other data. Secure Hash Algorithm Version 1, or SHA 1, is a mathematical algorithm. SHA 1 was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA). The United States of America has adopted the SHA 1 hash algorithm described herein as a Federal Information Processing Standard. It is computationally infeasible (2^160th) to find two different files that produce the same SHA 1 value. This allows investigators to identify a file by the value, regardless of the name of the file beyond 99.99 percent certainty. The SHA 1 digital signature can be explained as a digital fingerprint, or DNA of the file.

u. "Compressed file" refers to a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.

v. "National Center for Missing and Exploited Children (NCMEC)" The Center provides information to help locate children reported missing (by parental abduction, child abduction, or running away from home) and to assist physically and sexually abused children. In this resource capacity, the NCMEC distributes photographs of missing children and accepts tips and information from the public. It also coordinates these activities with numerous state and federal law enforcement agencies.

w. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

7. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

8. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage and social networking.

9. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

10. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

11. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

12. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Google, Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

13. As is the case with most digital technology, computer communications can be saved or stored on hardware, and computer storage media are used for these purposes. Storing this information can be intentional, (i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). However, digital information can also be retained unintentionally, (e.g., traces of the path of an electronic communication may be automatically stored in many places such as temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner can often recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained for long periods of time until overwritten by other data.

14. The interaction between software applications and the computer operating systems often results in material obtained from the Internet being stored multiple times, and even in different locations, on a computer hard drive without the user's knowledge. Even if the computer user is sophisticated and understands this automatic storage of information on his computer's hard drive, attempts at deleting the material often fail because the material may be automatically stored multiple times and in multiple locations within the computer media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's computer media, despite, and long after, attempts to delete it. A thorough search of this media could uncover evidence of receipt, distribution, and possession of child pornography.

15. Data that exists on a computer is particularly resilient to deletion. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the file is sent to the recycle bin, where it can be easily accessed by the user. Even when a person deletes a file from the recycle bin, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are

overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residues of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE

16. On June 10, 2017, the FBI received a report to the FBI Public Access Line (PAL) Unit regarding the possession and distribution of child pornography by Christopher MAYHALL, of Dublin, TX. The tip was submitted in an online tip to the FBI PAL Unit via tips.fbi.gov with the following text sent in the complaint:

> "Christopher David MAYHALL, Age: 40 DOB [redacted]/77 uses the social media app Kik (inradax77) to contact other members of child porn and pedophilia groups to exchange child pornography outside as well as inside of Kik. Dropbox for android is used to exchange videos of child porn, his Google Drive app is full of child porn, his LG V20 is full of child porn. Inradax77@gmail.com is the google account associated with the child porn. I personally have seen contents dating back a few years in his storage. He lives at 520 W Oneil St. unit B in dublin tx. He has family and friends as well as informants within local law enforcement, he has made terroristic threats against myself, as well as towards me regarding my family namely my 2yr old neice. He sells prescription drugs, and methamphetamines from Granbury to Brownwood. Hos phone number is [redacted]-2069. He has commented via text message to me that as of today 6/10/17 he will do everything in his power (including but not limited to the life of my 2yr old neice) to cause me suffering. He is on facebook as christopher mayhall, he has already had one account disabled for attempting to send child pornography to my cell phone via messenger in an attempt to "get me". He has been successful in evading law enforcement for years, he claims.

> He has a drop in the bathroom floor of his house that he can easily dispose of anything in the event of a raid. If there is any information i can provide further, please contact me on my cell phone, if/when necessary."

17. Between June 2017 and February 2018 agents attempted to locate and interview the complainant listed on the PAL Unit tip on several occasions. Agents talked to family members of the complainant but ultimately were unable to locate and speak to the complainant.

18. Due to the inability to locate and speak with the initial complainant, a knock and talk was determined to be the most appropriate course of investigative action. Therefore, on April 25, 2018, FBI SA Jacob Downing and Abilene Police Department (APD) Detective Christopher Milliorn conducted a knock and talk with Christopher MAYHALL at his residence, 520 W. Oneil St., Dublin, TX. During the knock and talk, MAYHALL stated he lived at the address and primarily stayed in the secondary house on the property. However, during the conversation, MAYHALL entered and exited the main residence to retrieve a cellular telephone.

19. Additionally, MAYHALL stated he knew Detective Milliorn and SA Downing were speaking with him because of a child pornography allegation. MAYHALL denied possessing any child pornography. He admitted he had seen child pornography after swapping his cellular telephone with a friend. MAYHALL would not give Detective Milliorn consent to search his cellular telephone without a warrant. Additionally, MAYHALL called his attorney while speaking with Detective Milliorn and SA Downing.

MAYHALL relayed that his attorney advised him to stop answering questions and ask Detective Milliorn and SA Downing to leave. Detective Milliorn and SA Downing subsequently left.

20. On or about October 21, 2018, an FBI agent acting in an undercover capacity (the "UC") posted an advertisement on a public messaging forum located on the internet, a means and facility of interstate and foreign commerce. The advertisement used language that is commonly associated with individuals seeking children for sexual purposes. The advertisement was titled "younger uncle" and stated the following: "young uncle, looking for like minded, no limits, kik me." Additionally, the advertisement listed a texting application with a user name for the UC so that individuals could contact the UC, and further stated that the UC would "love to meet others with similar taboo interests..."

21. On or about November 1, 2018, the UC received a message from username "inradax77" on the texting application that indicated he read the post and asked the UC "Your a naughty uncle."

22. Since November 1, 2018, the UC has been acting in an undercover capacity communicating with the user "Inra Dax 77", identified as Christopher MAYHALL. During the course of the messaging conversations, MAYHALL provided the telephone number [redacted]-2069 to the UC. After receiving MAYHALL's telephone number, UC had numerous recorded telephone conversations with MAYHALL, wherein he identified himself as "Chris." MAYHALL also utilized the screen name "DirtyTexan77" to communicate with the UC via the application Telegram.

23. MAYHALL has stated on multiple occasions he was interested in having sex with a young boy and believes the UC to have an 11 year old nephew. MAYHALL has requested the writer to send nude photographs and videos of the child as well as images and videos of the child engaged in sexual acts with the UC. During their conversations, MAYHALL sent, "take a pic with his hands on your cock and yours his and touch his hole."

24. MAYHALL attempted to set up a meeting with the UC and the 11 year old nephew to engage in sexual activities. MAYHALL also introduced the UC to a second subject, only known as "Danny," who also requested to meet to engage in sex with a child. "Danny" was interested in meeting the UC to engage in sex with a young girl and "Danny" believed the UC to have an 8 year old niece. "Danny" agreed to exchange methamphetamine with the UC for sex with the two children when he and MAYHALL met the UC in Midland, Texas. Upon setting up the meeting, MAYHALL informed the UC, he and "Danny" got into a car accident and asked if the UC could come to his residence with the 11 year old boy.

25. On December 16, 2018, MAYHALL sent a video to the UC of an infant being sexually assaulted by an adult male. The video is approximately 12 seconds in length and shows an infant boy with an adult male attempting to anally rape the infant boy with an erect penis.

26. During the conversations with the UC, MAYHALL indicated he had been sexually active with minor children. The UC asked, "You been with young a lot??" MAYHALL responded with, "About 6 you're the first in Texas it seems real."

27. When asked what his favorite age would be MAYHALL sent, "Alll, 3 or4 to 14, 7 8 9, Can't just pick one."

28. Subscriber information associated with telephone number [redacted]-2069 identified MAYHALL's father, David Lee Mayhall, as the financially liable party, living as 520 W. Oneil St., Dublin, TX.

29. On January 30, 2019, MAYHALL was indicted by a Grand Jury sitting in the Western District of Texas. MAYHALL was indicted on one count of Sexual Exploitation of Children – Attempted Production of Child Pornography, 18 U.S.C. § 2251(a) and (e), and one count of Distribution of Child Pornography, 18 U.S.C. § 2252A(a)(2) and (b)(1).

30. On January 31, 2019, FBI Special Agents learned from Agents with the U.S. Postal Inspector Service that Christopher David MAYHALL regularly receives mail at 520 W. Oneil St., Dublin, TX, and this mailing address is current as of January 30, 2019.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

31. Based upon my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

a. Child pornography collectors view children as sexual objects. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Collectors of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica[1], and videotapes for many years.

d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format, such as hard drives, diskettes, and CD-ROMs, in a safe, secure and private environment, including their home, car and other areas under their control. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

[1] "Child erotica," as used in this affidavit, is defined as materials or items that are sexually arousing to certain individuals but which are not in and of themselves obscene or do not necessarily depict minors in sexually explicit poses or positions. Such material may include non-sexually explicit photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), drawings, or sketches, written descriptions/stories, or journals.

e. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Collectors of child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. Child pornography collectors go to great lengths to conceal and protect from discovery their collection of sexually explicit images of minors. They may have passwords to access programs or control encryption written down either in the vicinity of their computer, or on their person, for instance, in their wallet or an address book.

h. Collectors of child pornography maintain images of minors with whom they have had sexual contact. If a picture of a minor is taken by such a person depicting the minor in the nude, there is a high probability the minor was used to produce sexually explicit images to be traded with people with similar interests.

32. Based on this investigation, Christopher MAYHALL, living at 520 W. Oneil St., Dublin, TX 74664, exhibits the common characteristics described above of someone involved in the distribution, transportation, receipt, possession and collection of child pornography, or the attempted distribution, transportation, receipt, or possession of child pornography. Christopher MAYHALL at 520 W. Oneil St., Dublin, TX 74664, maintains at least one file recognizable as child pornography and has shared it via cellular telephone. Additionally, Christopher MAYHALL has expressed to UC FBI Special Agents an interest in child pornography and has attempted to solicit child pornography from the UC FBI Special Agents. Based on these facts and those set forth in the Background of the Investigation it is believed that Christopher David MAYHALL demonstrates the characteristics of a collector of child pornography.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

33. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard drives, diskettes, tapes, laser disks, Bernoulli drivers and others) store the equivalent of thousands of pages of

information. Especially when a user wants to conceal criminal evidence, he or she may store it in random order with deceptive file names.

This requires search authorities to examine all the stored data to determine whether it is included in the warrant. This examination process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill in a properly controlled environment. The vast array of computer hardware and software available today requires even computer experts to specialize in some systems and applications. It is difficult to know before a search which expert should analyze the system and its data. A search of a computer system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover hidden, erased, compressed, password-protected, and other encrypted files. Because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

34. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices, as well as the central processing unit ("CPU"). In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored

on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices.

35. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment. Peripheral devices, which allow users to enter and retrieve data from stored devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly retrieve the evidence sought.

36. In addition to being evidence of a crime, in cases of this sort, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, printer, modem and other system components were used as a means of facilitating a criminal violation and should all be seized on that basis alone. Accordingly, permission is sought herein to seize and search computers and related devices consistent with the scope of the requested search.

37. In my training and experience, persons conducting electronic transactions via computers and the Internet, routinely print hard copies of such documents, to memorialize the transaction.

38. Lastly, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

CONCLUSION

39. During the course of a law enforcement investigation, Christopher MAYHALL has attempted to get the UC to produce child pornography on multiple occasions. Furthermore, MAYHALL has distributed child pornography to the UC. MAYHALL has shown he has a sexual interest in children and child pornography. As stated above, collectors of child pornography rarely, if ever, dispose of sexually explicit images of minors because the images are treated as prized possessions.

They have been known to store such images in different formats including digital media. They have been known to store such images in different places including their home, their car, and other areas under their control. MAYHALL has indicated he has had sexual contact with minors, and individuals with a sexual interest in children maintain images of minors with whom they have had sexual contact. If a picture of a minor is taken by such a person depicting the minor in the nude, there is a high probability the minor was used to produce sexually explicit images to be traded with people with similar interests.

40. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of such criminal offenses may be located at the premises described in Attachment A, in violation of Title 18 U.S.C. Sections 2251, 2252, 2252A and that the violations have occurred and continue to occur at 520 W. Oneil St, Dublin, TX.

41. I, therefore, respectfully request that attached warrant be issued authorizing the search of 520 W. Oneil St, Dublin, TX and the person of Christopher David MAYHALL (more fully described in Attachment "A") and the seizure of evidence (more fully described in Attachment "B").

Respectfully submitted,

Jacob R. Downing
Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence this 31st day of January, 2019, at 1:30 p.m. in Fort Worth, Texas.

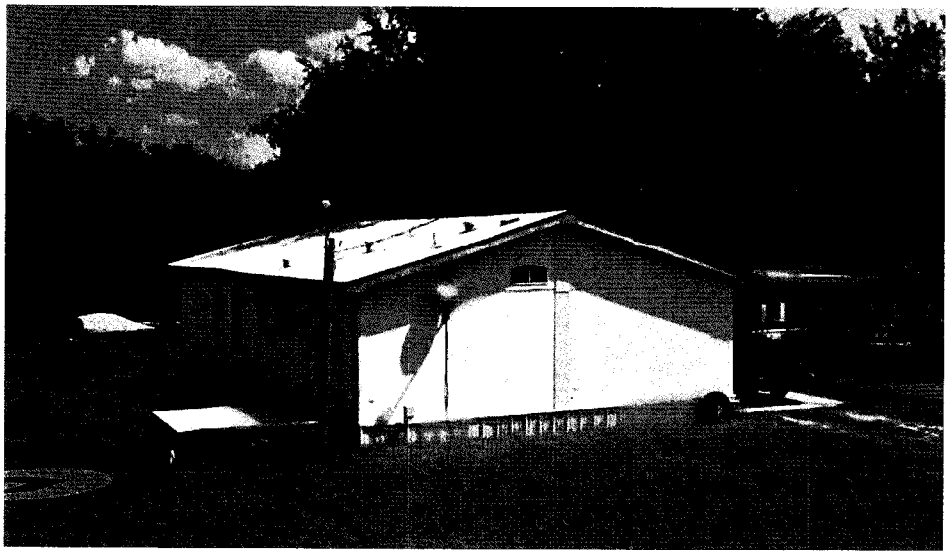
JEFFREY L. CURETON
United States Magistrate Judge

ATTACHMENT A

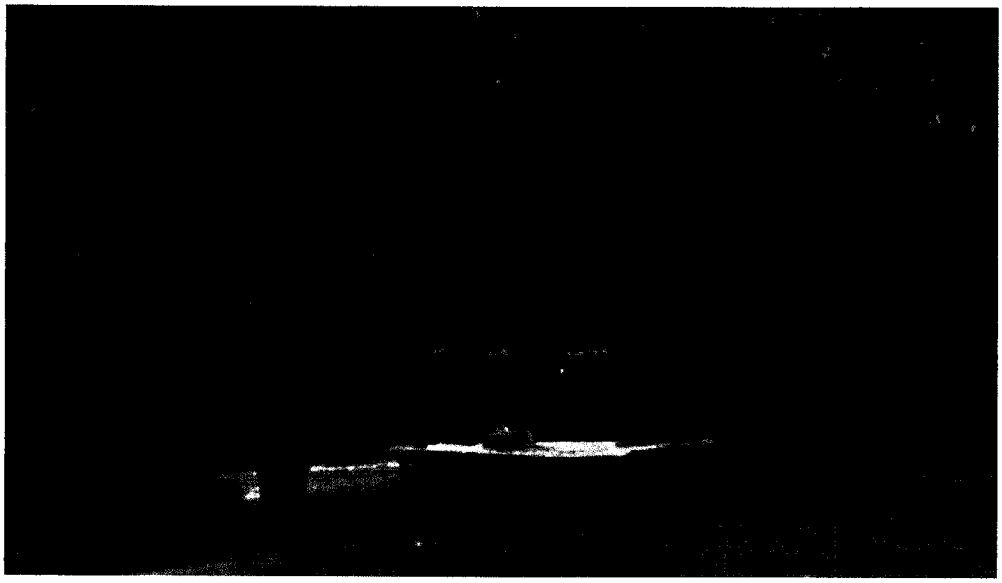
DESCRIPTION OF THE PREMISES AND PERSON TO BE SEARCHED

The entire property located at 520 W. Oneil St., Dublin, TX 76446, including any residential building, any outbuildings, any appurtenances thereto, and any vehicle located on the premises or its curtilage. The property is described as having two residential buildings on the premises.

The main residence is described as a one story, white sided house with white trim, a white shingled roof, and a single car port in rear of the residence. The numbers "520" can be seen on the outside wall of the home, on the south side of the building.



The secondary residence is described as a one story, green sided house with white trim, a white singled roof and a covered patio in the front. There are no independently identifiable numbers or letters on the house distinguishing it from the main residence.



The person of Christopher David MAYHALL, DOB [redacted]-1977.

Any and all computers and storage media found therein, as further described by Attachment B.

Attachment A

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252, 2252A, et al:

1. Computers or storage media used as a means to commit the violations described above.

2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

   a. Computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

b. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

c. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

d. evidence of the lack of such malicious software;

e. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

f. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

g. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

h. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

i. evidence of the times the COMPUTER was used;

j. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

k. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

l. records of or information about Internet Protocol addresses used by the COMPUTER;

m. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

n. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography and child erotica.

5. Records, information, and items relating to violations of the statutes described above including:

a. Records, information, and items relating to the occupancy or ownership of the PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence, rental or lease agreements, mortgage documents, rental or lease payments and credit card information, including, but not limited to, bills and payment records.

b. Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;

c. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

d. Records and information relating to the sexual exploitation of children, including correspondence and communications between users of the website described in the warrant application.

e. Records and information showing access to and/or use of the website described in the warrant application.; and

f. Records and information relating or pertaining to the identity of the person or persons using or associated with Inradax77@gmail.com, Inra Dax77, "Dirty Texan 77, and any other pdeudonymns or usernames utilized by MAYHALL.

g. Records and information relating or pertaining to the ownership of telephone number 254-495-2069

6. Any and all notes, documents, records, computer files or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), including communications

between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography or membership in online groups, clubs, or services that provide or make accessible child pornography to members.

7. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

8. Any and all cameras, film, videotapes or other photographic equipment that may be used to commit or facilitate commission of violations of 18 U.S.C. §§ 2251, 2252 and 2252A.

9. As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

10. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical,

arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

11. The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.